Guest Commentary

State's 'cyber security' a constant challenge

By Thomas M. Jarrett

"The security of Delaware's information technology system is critical to the well-being of our state as a whole — not just the business of the state, but also its economy."

— Thomas M. Jarrett

At the invitation of Sen. Tom Carper, D-Del., I was recently honored to testify before the Subcommittee on Federal Financial Management, Government Information and International Security of the U.S. Senate's Committee on Homeland Security and Government Affairs.

I spoke in two capacities, first representing the great state of Delaware as secretary of Delaware's Department of Technology and Information, and second, as the current president of the National Association of State Chief Information Officers, or "NASCIO."

The topic of the hearing was "Securing Cyberspace: "Efforts to Protect National Information Infrastructures Continue to Face Challenges." This column summarizes the substance of my testimony and explains why "cyber security" is important to each and every one of us.

While this may sound like the title of a very boring and long textbook, cyber security is important to every Delawarean today. If you use a credit card, have a bank account, and especially if you use a computer for e-mail or to go onto the Internet, your name and much of your personal information is out in cyberspace. That means that nearly all financial records today are kept on computers, whether or not you personally use a computer yourself.

As Delaware's CIO in charge of all state government information and communications technology, my highest priority is cyber security. The security of Delaware's information technology system is critical to the well-being of our state as a whole — not just the business of the state, but also its economy. A secure technology system also is critical to making certain that our first responders have access to the vital information that they need in times of emergency.

In the simplest terms, keeping those who would wish to do us harm out of our network and systems is the primary challenge of IT (information technology) security staff in Delaware and across the nation. Delaware's state network may be small in comparison to some other states, yet we're responsible for over 130,000 users representing all three branches of government including our law enforcement, first responder and educational communities.

In 2004 we processed 84 million pieces of inbound e-mail for state users. We've deployed new software that permits us to track network events on a daily basis and we fend off nearly 3,000 daily attempts at entering our network. Let me repeat that again — *nearly 3,000 attempts a day to invade our network.* Imagine this number multiplied by the number of attempts that are also occurring against universities, banks and credit companies on a daily basis and you can begin to see that "keeping the bad guys out" is a daily challenge for everyone working in the area of information technology security.

Because of our extreme diligence, we have not had a significant intrusion into our state network. Keeping those who would wish to do us harm out of our network requires multiple layers of protection. While it is rarely a terrorist in the traditional sense of the word who threatens a state network, we do not focus specifically on who is trying to infiltrate our network. Rather, our goal is to keep all those with bad intentions from ever entering our system.

Without lapsing into too many technical terms, we use a number of different hardware and software products to protect our network. We search for viruses, spam, spyware and other recognized problems. Delaware is proactive in establishing collaborative partnerships at the federal and local levels. We have a working relationship with the FBI, which performs vulnerability audits and scans for us. We collaborate with the private sector too; Delaware was the first state to become part of a security cooperation agreement with Microsoft.

During times of heightened security alerts like that resulting from the recent terror incidents in London, we raise the bar on cyber security. We increase our vigilance and our monitoring because we are well aware that a virus that begins in Asia can travel to the U.S. in a matter of a few short hours. In a very short period of time, it is possible for a system that has not been secured or properly maintained to be completely overrun.

What does the future hold? Unfortunately, I have to share that I believe that threats to cyber security will only increase and we will face continual attacks and attempts on multiple fronts. State IT officials must continually adjust how and what gets filtered, blocked or monitored. New threats appear almost daily and they can, in a matter of seconds, render services we've all come to depend upon like e-mail and the Internet completely unusable. In the worst case scenario, without proper protection, an attack could potentially cripple or completely shut down an entire state government.

We all must understand that all critical infrastructure is the same by its very nature — *critical* — whether it is a roadway system or an information network. Infrastructure is about moving people and information, and a state's network infrastructure is equally as important as its highways, electric power grid, or mass transit system.

On the national level, as president of NASCIO, we are working with the states to get a comprehensive picture of the challenge that cyber security represents. We have produced a series of "snapshots" into what a few states are doing.

Let me share a few experiences from my state colleagues. Michigan reports that nearly 32 percent of its incoming e-mail carries viruses, while Montana reports a rise from 93 attempted virus infections in 1997 to nearly 45 million in 2005; Kansas blocked 600,000 intrusion attempts over a three- to four-hour period during one recent attack.

Protecting critical information technology infrastructure does not come cheaply. We estimate that my department spends $5 million, or 15 percent of our annual budget, annually on security.

NASCIO points out that information systems in general are the only part of the nation's critical infrastructure that is under attack everywhere, all the time — and these attacks are inflicting millions of dollars in damage. Cyber attacks — even those without terroristic intent — could disrupt governments' operations in general or homeland security mission-critical systems specifically. It is our duty to secure these systems from all types of threats, regardless of the intent behind them and as soon as possible.

While these threats are ongoing and will continue, there are things that all of us can do to help to secure our own information and avoid identify theft loss. Anyone using a computer to conduct personal business, such as banking, shopping or paying bills online, should be diligent in checking account statements for unusual or unauthorized activity. Under no circumstances should anyone ever provide personal or financial information in response to an unsolicited e-mail.

A relatively new cyber threat called "phishing" consists of unauthorized persons creating Web sites that look exactly like the Web site of a bank or credit card company, or even eBay or Amazon. These false sites will often ask for a credit card number, bank account or Social Security number. No reputable organization will request personal information in this fashion and unsolicited e-mails are best deleted without opening the item or responding in any manner.

When in doubt regarding the possibility of cyber fraud, the Delaware attorney general's Office of Consumer Fraud is available for consultation and reporting of cyber fraud incidents.

As CIO responsible for the security of Delaware's network, I welcome this opportunity to highlight the status of our security efforts and am committed to the protection of Delaware's vital information technology resources.

EDITOR'S NOTE: Thomas M. Jarrett is secretary of the Delaware Department of Technology and Information. He can be reached at 739-9500.